UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,504	08/18/2003	Naoki Matsuhira	122.1562	1724

21171 7590 05/31/2011

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
05/31/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/642,504	MATSUHIRA, NAOKI	
	Examiner	Art Unit	
	FARID HOMAYOUNMEHR	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *28 March 2011*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 8/18/2003; amendment filed 3/28/2011.

2. Claim 15 is new.

3. Claims 1-14 are cancelled by the applicant.

4. Claim 15 is pending and examined.

Response to Arguments

5. Applicant's argument regarding prior art rejection is not persuasive. Applicant argues:

> "That is, the Action looks to packet encryption of Arrow and asserts that Arrow teaches that because the filter information is in the packet the filter information is encrypted
>
> Claim 15 states:
>
> a packet transmitting apparatus, at a sending side, to provide a filter key for identifying a specific value of showing a VoIP performing a VoIP communication,

bury the provided filter key in an IPv6 extended header added to an IPv6 header or in a flow label region in an IPv6 header or the transferred packet to prevent the filter key from being encrypted by an IPsec and transmit the packet with the filter key to a receiving side

That is, claim 15 makes it clear that the packet transmitting apparatus or transmitter does not encrypt the filer key ("prevent the filter key from being encrypted") and the packet is transmitted with the unencrypted filter key ("transmit the packet with the filter key to a receiving side")."

However, as indicated in the rejection, the authentication information is put in the header and accessed before decryption (see Arrow col. 12 lines 35-46). Therefore, it shows that the packet is encrypted, but the header part including the authentication information is not encrypted. Therefore, as required by the claim, the key information (authentication data) is not encrypted in Arrow.

Accordingly, applicant's argument is found non-persuasive.

Note the new rejection under section 112.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claim includes:

> "a packet transmitting apparatus, at a sending side, to provide a filter key for identifying a specific value of showing a VolP performing a VolP communication, bury the provided filter key in an IPv6 extended header added to an IPv6 header or in a flow label region in an IPv6 header or the transferred packet to prevent the filter key from being encrypted by an IPsec and transmit the packet with the filter key to a receiving side;"

The exact meaning of bury the key in the header is not understood. For the purpose of this examination, it is assumed that it means including the key in the header of the packet, but the claim is indefinite as the word "bury" can have other meanings other than simply including a value within a field.

Also, prevent the filter key from being encrypted by an IPsec is interpreted to mean that the packet is protected using an IPsec protocol, which encrypts at least part of the packet, but the key is not encrypted. The claim language does not capture the exact same.

The claim also includes:

> "a packet receiving apparatus, at the receiving side, to receive the encrypted packet,"

However, as mentioned above, it is not clear if the claim the packet is encrypted the step mentioned above. Accordingly, there is no antecedent basis for "the encrypted packet". As mentioned above, for the purpose of this examination, it is assumed that part of the packet is encrypted using the IPsec protocol to secure the packet.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Christensen (US Patent No. 7'292'530, filed Dec. 29, 2000), hereinafter called Chris,) in view of Arrow et al. (US Patent No. 6'154'839, dated Nov. 28, 2000).

7.0. As per claim 15, Chris is directed to a packet communication system performing a VoIP communication, at least, therein where a transferred packet is filtered, said packet communication system comprising:

a packet transmitting apparatus, at a sending side, to provide a filter key for identifying a specific value of showing a VoIP performing a VoIP communication (Chris is directed to a method of improving network performance by recognizing high priority packets from information in the packet header, and process high priority packets accordingly. In particular, Chris col. 8 lines 25 to 43 shows VoIP packets are recognized (filtered) from header information and given higher priority Also, Chris col. 10 line 63 to col. 11 line 10 shows that the operating parameter in the header is a VoIP identifier. Therefore, Chris teaches filtering information is used to identifying a specific value showing a VoIP performing a VoIP communication, and uses this information to prioritize the service)

Chris clearly teaches applying his invention to TCP/IP packets as example (see col. 2 lines 130-40), but does not explicitly teach, bury the provided filter key in an IPv6 extended header added to an IPv6 header or in a flow label region in an IPv6 header or the transferred packet to prevent the filter key from being encrypted by an IPsec and transmit the packet with the filter key to a receiving side.

However, Arrow is directed to a packet filtering method characterized by storing filtering information for use in filtering at a receiving side in an encrypted packet to be sent to the

receiving side and sending it from a sending side (col. 6 lines 46-60 shows the encryption and authentication information is added to a packet at sending side, and verified at the receiving side. In addition, col. 12 lines 35-46 show that packets are decrypted after they are authenticated, and therefore, it shows packets were encrypted. Also Arrow teaches that if the packets are not authenticated they are filtered out), wherein an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6 (Fig. 8 and associated text shows the filtering data is placed in the address field of a packet. Arrow Fig 9 and associated text shows that user ID information, which is used for authentication (filtering) is put in the header of a packet. Address field of packets, such as IP packets are in the packet header. Column 6 lines 21-35 teach IP packets as examples for implementation of invention. It also explicitly teaches to use the technique regardless of the current version of IP protocol (col. 6 lines 30-35), which was Ipv6 at the time of invention. Ipv6 was well known at the time of invention. Therefore, Arrow teaches putting filtering information in a header of a packet and also suggests using IP packets for implementation. Therefore, Arrow makes it obvious to bury the provided filter key in an IPv6 extended header added to an IPv6 header or in a flow label region in an IPv6 header or the transferred packet to prevent the filter key from being encrypted by an IPsec and transmit the packet with the filter key to a receiving side.

Also, as mentioned above, Arrow teaches authenticating the packet before decrypting it. Therefore, the authentication information (filtering info) was not encrypted). In addition,

IPsec was a known protocol at the time of the invention. A version of IPSec, called ESP has a mode in which the packets are only protected for authentication (see description of IPSec in Wikipedia at http://en.wikipedia.org/wiki/IPsec. Accordingly, IPsec can protect for authentication without encrypting the packet, which would accomplish the claim requirement that the key that is not encrypted.

At the time of invention, it would have been obvious to the one skilled in art to enhance Chris' system by including security features as described by Arrow's system which stores filtering information in the header of an encrypted packet. The motivation to do so would be enhancing the security of the packets as stated by Arrow in the system of Chris (e.g. abstract) which enhances the quality of service of the network by prioritizing more sensitive packets such as VoIP packets.);

a packet receiving apparatus, at the receiving side, to receive the encrypted packet, except for the filter key, from the sending side through a network between a server and a client, hold predetermined filtering information of the receiving side and compare the filtering information with the filter key detected from the received pack et at the receiving side (see Arrow figures 2,3 and 9 where the received packet is authenticated); and

an authentication apparatus for receiving user authentication information input from a user receiving filtering service, authenticating the user, and assigning and distributing a filter key to said packet transmitting apparatus, which filter key corresponds to the user

authentication information, after the authentication (Arrow col. 6 lines 46-60, showing that the authentication data is added to each packet. Also, performing packet authentication verification based on information within he packet (which is performed by Arrow as shown above) requires that the authentication data is added to the packet at the sending site).

[Claims 2, 4, 5, 8-10, 12 and 13 are cancelled. The associated rejection is reproduced for the record:

7.1. As per claims 8-10, Arrow is directed to a packet filtering method characterized by storing filtering information for use in filtering at a receiving side in an encrypted packet to be sent to the receiving side and sending it from a sending side (col. 6 lines 46-60 shows the encryption and authentication information is added to a packet at sending side, and verified at the receiving side. In addition, col. 12 lines 35-46 show that packets are decrypted after they are authenticated, and therefore, it shows packets were encrypted. Also Arrow teaches that if the packets are not authenticated they are filtered out), wherein an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header is used to transmit the filtering information as to prevent the filtering information from being encrypted, when the packet is a packet in compliance with Ipv6 (Fig. 8 and associated text shows the filtering data is placed in the address field of a packet. Arrow Fig 9 and associated text shows that user ID

information, which is used for authentication (filtering) is put in the header of a packet. Address field of packets, such as IP packets are in the packet header. Column 6 lines 21-35 teach IP packets as examples for implementation of invention. It also explicitly teaches to use the technique regardless of the current version of IP protocol (col. 6 lines 30-35), which was Ipv6 at the time of invention. Ipv6 was well known at the time of invention. Therefore, Arrow teaches putting filtering information in a header of a packet and also suggests using IP packets for implementation. Therefore, Arrow makes it obvious to put the filtering information in the header of an Ipv6 packet header. Also, as mentioned above, Arrow teaches authenticating the packet before decrypting it. Therefore, the authentication information (filtering info) was not encrypted);

said filtering information is used to identifying a specific value showing a VoIP performing a VoIP communication (Arrow does not explicitly teach said filtering information is used to identifying a specific value showing a VoIP performing a VoIP communication. Chris is directed to a method of improving network performance by recognizing high priority packets from information in the packet header, and process high priority packets accordingly. In particular, Chris col. 8 lines 25 to 43 shows VoIP packets are recognized (filtered) from header information and given higher priority Also, Chris col. 10 line 63 to col. 11 line 10 shows that the operating parameter in the header is a VoIP identifier. Therefore, Chris teaches filtering information is used to identifying a specific value showing a VoIP performing a VoIP communication, and uses this information to prioritize the service. At the time of invention, it would have been obvious

to the one skilled in art to enhance Arrows system which stores filtering information in the header of an encrypted packet by including filtering information to filter VoIP packets as taught by Chris. The motivation to do so, is as stated by Chris (e.g. abstract) would be to enhance the quality of service of the network by prioritizing more sensitive packets such as VoIP packets.);

and the specific value showing the VoIP provides a first function of the filtering and a second function of having a communication partner recognize the VoIP, simultaneously (As discussed above, and in col. 7 lines 9-30, Arrow teaches a filtering system that filters packets based on specific values in the packet headers. The combination of Arrow and Christensen makes it obvious to filter VoIP packets based on a specific VoIP identifier in the packet header. Christensen teaches using that specific VoIP parameter to set the operational parameters, and therefore recognize the VoIP communication. Therefore, Arrow in view of Christensen makes it obvious to use the VoIP identifier to do both the filtering function and having a communication partner recognize the VoIP, simultaneously). Note that per col. 12 lines 20-35, the user is authenticated in advance and have received proper authentication information to include in the packet user ID field. This authentication information is used by the firewall to authenticate user's packet. Note also that the functionality and hardware required to hold the filter keys and storing them is inherent to Arrow's system. Also note that Arrow col. 7 lines 40-55 teach that the equipment is provided with a buffer for temporarily storing a received packet passing through the filter key detecting unit and in that the

comparing function unit is comprised of a filter key table holding a predetermined plurality of different filter keys.

7.2. As per cancelled claim 2, Arrow in view of Chris is directed to a packet filtering method characterized by, receiving an encrypted packet at the receiving side, from a sending side, detecting filtering information stored in that packet (see response to claim 1), holding predetermined filtering information of the receiving side, comparing filtering information of the sending side detected from the packet with the filtering information of the receiving side, and, when the two do not match, discarding that packet (for example, col. 8, lines 4-23, or col. 6, lines 45-60), wherein an Ipv6 extended header added to an Ipv6 header or in a flow label region in an Ipv6 header, is used to transmit the filtering information so as to prevent encrypting the filtering information when the packet is a packet in compliance with Ipv6, wherein said filtering information is used to identify a specific value showing a VoIP performing VoIP communication (see response to claim 1).

7.3. As per cancelled claim 4, limitations of claim 4 are substantially the same as claim 1, and note that the comparing function unit is equivalent to the authenticating unit of Arrow as shown in col. 12 line 21-34.

7.4. As per canceled claim 5, Arrow in view of Chris is directed to a communication equipment as set forth in claim 4, characterized in that: the equipment is provided with a buffer for temporarily storing a received packet passing through the filter key detecting unit and in that the comparing function unit is comprised of: a filter key table holding a predetermined plurality of different filter keys (col. 7, lines 40-55), a search unit for searching if there is a filter key matching with a filter key detected by the filter key detecting unit in the filter key table and when there is none, outputting a discard command, and a buffer control unit for receiving the discard command and controlling the system so as to discard the packet stored in the buffer (see response to claim 3).

7.5 As per cancelled claim 12, Arrow in view of Chris is directed to a communication equipment as set forth in claim 4, wherein an authentication apparatus is further included, the authentication apparatus having: a filtering authentication function unit for receiving user authentication information input from a user receiving a filtering service and authenticating the user (Arrow col. 7 lines 30-40); and a filter key providing function unit for assigning and distributing said filter key to be stored in a packet corresponding to the user authentication information to the user after the authentication at the filtering authentication function unit (Arrow's claim 4 and also see Fig. 9 and associated text).

7.6. As per cancelled claim 13, Arrow in view of Chris is directed to a communication equipment as set forth in claim 12, wherein said filtering authentication function unit has: a user authentication database in which user authentication information is

registered in advance, and a decision unit for determining the veracity of the input user authentication information by referring to the user authentication database; and said filter key providing function unit has: a filter key assigning table holding said filter key assigned in advance corresponding to user authentication information, and a filter key sending unit for sending a corresponding filter key from the filter key assigning table to the user when the veracity is confirmed (Arrow col. 12 line 2 to 63 shows an embodiment where the authentication data is readily stored in the Address Translation Unit, where the data is used to authenticate the user (Also see Arrow claim 4). Arrow Fig 4 and 5 show use of a database to store information processed by the system, and a command module for executing commands received. A database stored information in tables, and once queried for a data item searches the tables for a match and provides the queried information. Note that to perform authentication, the authentication information must be stored and made available to the authenticating system).]

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Farid Homayounmehr/

Primary Examiner

AU 2434

5/27/2011